Remarks

Claims 1-19 are pending.

Rejections Under 35 U.S.C. § 103(a)

The Examiner rejects Claims 1-19 on the ground of being unpatentable over "A Decentralized Model for Information Flow Control" (Myers et al.) and "VISA: Netstation's Virtual Internet SCSI Adapter" (Van Meter et al.).

Myers et al. discloses a model for controlling information flow in systems with mutual distrust and decentralized authority. The model allows users to share information with distrusted code (*e.g.*, downloaded applets), yet still control how that code disseminates the shared information to others. The model purports to improve on existing multilevel security models by allowing users to declassify information in a decentralized way, by improving support for fine-grained data sharing, and by allowing users to control the flow of their information without imposing the rigid constraints of a traditional multilevel security system.

Myers et al. discloses that when a computational environment contains many trusted nodes connected by a network, the communication links between the nodes must be trusted, which can be accomplished by encrypting communication between nodes. Myers et al. also discloses that information flow control is vital for large or extensible systems. In a small system, preventing improper propagation of information is easy: you don't pass data to code whose implementation is not completely trusted. This simple rule breaks down in larger systems, because the trust requirement is transitive: any code the data might travel to must also be trusted, requiring complete understanding of the code. As the system grows larger and more complex, and incorporates distrusted code (*e.g.*, web applications), complete trust becomes unattainable.

As shown in Figure 2 of Myers et al., a bank serves many customers, each of whom would like to keep his data safe from other customers and non-customers. In addition, the bank stores private information, such as its current assets and investments, that it would like to keep safe from all customers and non-customers. In this banking example, the bank receives periodic requests from each customer, for example, to withdraw or deposit money. Each request should be able to observe only information that is owned by that customer, and none of the bank's private data. The bank is better than real banks in that it allows customers to control dissemination of their account information; each customer has a distinct information flow policy for his account information, which prevents the bank from leaking the information to another party.

Van Meter et al. discloses a Virtual Internet SCSI Adapter (VISA) to evaluate the performance impact on a host operating system of using IP to communicate with peripherals, especially storage devices. Connecting peripherals directly to a network allows sharing of resources and improves system configuration flexibility. Network clients can access peripherals, such as network-attached storage devices (NASDs), without the intervention of a server.

A Netstation project concentrates on operating systems, network protocols, hardware mechanisms, and security and sharing models for network-attached peripherals. Some of the goals of the project are to demonstrate: (1) that IP can provide acceptable performance in a host operating system when used to access peripherals, (2) that IP can be implemented efficiently inside network-attached peripherals, and (3) that a derived virtual device model enables efficient, secure use of network-attached peripherals (NAPS).

Netstation is a heterogeneous distributed system composed of processor nodes (CPU/Memory) and network-attached peripherals. The peripherals are attached to a shared Local Area Network as shown in Figure 1 of Van Meter et al. The peripherals include displays, magnetic disks, a RAM disk, a camera and a keyboard/mouse. Because the peripherals are attached to an open network with both trusted and untrusted nodes on the net, security at NAPS is critical. A model, referred to as a derived virtual device (DVD), provides a protected execution context at the device, allowing direct use of the devices by untrusted clients, such as user applications. The owner of a device defines the security policy, downloads a description to the NAP, and the NAP enforces the policy. This allows the owner to define a set of resources and operations allowed. Thus, a camera can be granted write access to only a specific region of a frame buffer, or a user application can be given read-only access to a DVD which represents a disk-based file or disk partition.

Claim 1 recites, *inter alia*, a method of enabling at least one functional block having an identifier for a controller having a unique identification. The method comprises encoding an enable code for the functional block of the controller based upon the unique identification of the controller and the identifier of the functional block; decoding the enable code for the functional block of the controller to obtain a decoded identification and a decoded identifier; and enabling the functional block of the controller when the decoded identification is equal to the unique identification and the decoded identifier is equal to the identifier of the functional block.

The Examiner states that Van Meter et al. does not teach "functional" in the context of the claims.

The Examiner further states that Myers et al. teaches "such 'functional' nature (page 131, the customer requests which are requests for functions such as transactions) for the motivation of decentralizing information control". The Examiner also states that each of: (1) "encoding an enable code for the [] block of said controller based upon the unique identification of said controller and the identifier of said [] block"; (2) "decoding the enable code for the [] block of said controller to obtain a decoded identification and a decoded identifier"; and (3) "enabling the [] block of said controller when said decoded identification is equal to said unique identification and said decoded identifier is equal to the identifier of said [] block" are taught by Van Meter et al. (page 72, "derived virtual device in which the set of types of access is set as policy by owner, also Figure 1"). These statements are respectfully traversed as applied to the refined recital of Applicants' claims.

As employed in the application, the term "encoding" means "encrypting, enciphering, or converting a set of intelligible information into a corresponding cipher coded set of information." Also, the term "decoding" means "decrypting, deciphering, or converting a cipher coded set of information into a corresponding set of intelligible information." *See* page 5, line 29 through page 6, line 3 of the specification.

It is submitted that nothing in Van Meter et al. teaches or suggests "encoding" or "decoding" as set forth in the refined recital of Claim 1. Van Meter et al., which teaches that a peripheral device, such as a camera, can be granted write access to only a specific region of a frame buffer or that a user application can be given read-only access to a disk-based file or disk partition, does not teach or suggest encrypting, enciphering, or converting a set of intelligible information into a corresponding cipher coded set of information, or decrypting, deciphering, or converting a cipher coded set of information into a corresponding set of intelligible information.

It is further submitted that nothing in Van Meter et al. teaches or suggests encoding an enable code for a block of a controller, decoding such enable code to obtain a decoded identification and a decoded identifier, and enabling such block of such controller when such decoded identification is equal to a unique identification of such controller and such decoded identifier is equal to an identifier of such block. Myers et al., which merely discloses that it is advantageous to encrypt communication between trusted nodes of a communication network, adds nothing to Van Meter et al. regarding any enable code for a block of a controller, obtaining an identification and an identifier from such enable code, and enabling a block of a controller when such obtained identification is equal to a unique identification of such controller and when such obtained identifier is equal to an identifier of such block.

Accordingly, the above reasons, Claim 1 patentably distinguishes over the references.

Claims 2-19 depend directly or indirectly from Claim 1 and patentably distinguish over the references for the same reasons.

The Examiner states that Claims 2, 3 and 5 recite limitations regarding "typical purchasing/selling situations". The Examiner states that purchasing and selling are well known in the art of e-commerce for the motivation of permitting transactions, and that Myers et al. (page 131) teaches banking e-commerce. These statements are traversed as applied to the refined recital of Applicants' claims, which do not recite "typical purchasing/selling situations". To the extent that the Examiner takes the position that the recitals of Claims 2, 3 and 5 are well known, then it is respectfully requested that the Examiner cite a reference within the context of Applicants' claims.

Since the references do not teach or suggest encoding or decoding an enable code, they clearly do not contemplate or suggest selling such enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block as set forth in Claim 2, or purchasing such enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block as set forth in Claim 3. Although Myers et al. teaches bank software and bank transactions, such as withdrawing and depositing money, there is no teaching or suggestion about purchasing or selling the recited "enable code" of Claims 1-3. Van Meter et al., which discloses peripherals on a local area network, adds nothing to Myers et al. in this regard. Therefore, it is submitted that Claims 2 and 3 further patentably distinguish over the references.

Furthermore, Claim 5 recites entering the identifier of the functional block and the unique identification of the controller into an encoder; encoding a purchase code as the enable code from the identifier of the functional block and the unique identification of the controller; and selling the purchase code.

Since the references do not teach or suggest encoding or decoding an enable code, they clearly do not contemplate or suggest entering an identifier of a functional block and a unique identification of a controller into an encoder, and encoding a purchase code as an enable code from such identifier of such functional block and such unique identification of such controller. Myers et al., which teaches bank software and bank transactions, such as withdrawing and depositing money, clearly does not teach or suggest selling such a purchase code that was encoded as an enable code. Van Meter et al., which discloses peripherals on a local area network, adds nothing to Myers et al. in this regard. Hence, it is submitted that Claim 5 further patentably distinguishes over the references.

Claims 6-9 and 16-18 are not separately asserted to be patentable except in combination with Claim 5 from which they directly or indirectly depend.

The Examiner states that Claims 10-14 recite limitations regarding typical software and hardware used in multi-level security systems. The Examiner further states that such software and hardware are well known in the art for the motivation of actuating e-commerce. The Examiner also states that Myers et al. (page 142) teaches a multi-level security system. These statements are traversed as applied to the refined recital of Claims 10-14, which recite additional limitations regarding the recited decoded identification, the recited decoded identifier, or the recited encoding step and the recited decoding step. Since the references do not teach or suggest the limitations of Claim 1, they clearly do not teach or suggest these additional limitations, which further distinguish over the references.

Furthermore, Claim 14 recites employing an encryption algorithm having a secret key as the encoding step; and employing a corresponding decryption algorithm having the secret key as the decoding step. It is submitted that the references do not teach or suggest employing any encryption algorithm having a secret key as the recited encoding step or employing any decryption algorithm having such secret key as the recited decoding step. To the extent that the Examiner takes the position that the recitals of Claims 1 and 14 are well known, then it is respectfully requested that the Examiner cite a reference within the context of Applicants' claims. Accordingly, it is submitted that Claim 14 further patentably distinguishes over the references.

Like Claims 2, 3 and 5, the Examiner states that Claims 15 and 19 recite limitations regarding "typical purchasing/selling situations". Again, those statements are traversed as applied to the refined recital of Applicants' claims, which do not recite "typical purchasing/selling situations". To the extent that the Examiner takes the position that the recitals of Claims 15 and 19 are well known, then it is respectfully requested that the Examiner cite a reference within the context of Applicants' claims.

Claims 15 and 19 depend directly or indirectly from Claims 1 and 14, include all of the limitations thereof, and patentably distinguish over the references for the same reasons.

Furthermore, Claim 15 recites employing a block number as the identifier of the functional block; employing a unique controller number as the unique identification of the controller; inputting the block number and the unique controller number into the encryption algorithm; outputting a purchase code as the enable code from the encryption algorithm; inputting the purchase code into the decryption algorithm; outputting a decrypted block number and a decrypted controller number from the decryption algorithm; and enabling the functional block of the controller when the decrypted block number is equal to the identifier of the functional block and the decrypted controller number is equal to the unique identification. The references do not teach or suggest the recited encryption algorithm, the recited enable code from such encryption algorithm, inputting the recited purchase code into the recited decryption algorithm, outputting a decrypted block number and a decrypted controller number from the recited decryption algorithm, and enabling a functional block of a controller when such decrypted block number is equal to an identifier of a functional block and such decrypted controller number is equal to a unique identification. Accordingly, Claim 15 further patentably distinguishes over the references.

Furthermore, Claim 19 recites displaying the unique controller number and the block number; informing a supplier of the unique controller number and the block number; and inputting the unique controller number and the block number into the encryption algorithm at a facility of the supplier. Since the references do not teach or suggest the limitations of Claim 15, they clearly do not teach or suggest these additional limitations, which further distinguish over the references.

For the above reasons, it is submitted that Claims 1-19 are in condition for allowance.

Reconsideration and early allowance are requested.

Respectfully submitted,

Kirk D. Houser
Registration No. 37,357
Attorney for Applicants

(412) 566-6083